Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of the Telecommunication	)	
Act of 1996:	)	CC Docket No. 96-115
	)	
Telecommunications Carriers' Use of	)	
Proprietary Network Information;	)	
	)	
Petition for Rulemaking to Enhance	)	RM-11277
Security and Authentication Standards		)
For Access to Customer Proprietary	)	
Network Information	)	

INITIAL COMMENTS OF THE TEXAS OFFICE OF PUBLIC UTILITY COUNSEL

The Texas Office of Public Utility Counsel, ("Texas OPC"), respectfully offers its initial comments, pursuant to the Federal Communications Commission's ("Commission" or "FCC") request for comment on what additional steps, if any, that the FCC should take to further protect the privacy of customer proprietary network information (CPNI) that is collected and held by telecommunication carriers pursuant to Section 222 of the Federal Telecommunications Act (FTA) of 1996.[1] Texas OPC represents the interests of residential and small commercial telephone customers before the Public Utility Commission of Texas, state and federal courts and the FCC.

[1] Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scattered sections of 15 and 47 U.S.C.) (FTA)

These initial comments address Texas OPC's views related to the care and control of CPNI information consistent with the policies set in FTA §222.

I. TEXAS OPC COMMENTS

OPC files its Initial Comments in response to the Commission's reaction to the petition filed by the Electronic Privacy Information Center (EPIC) expressing concerns about the sufficiency of carrier practices related to CPNI.[2] The EPIC petition indicates numerous websites that advertise the sale of personal telephone records for a price. Specifically, data brokers advertise the availability of cell phone records, which include calls to and/or from a particular cell phone number, the duration of such calls, and may even include the physical location of the cell phone. In addition to selling cell phone call records, many data brokers also claim to provide calling records for landline and voice over Internet protocol, as well as non-published phone numbers. In many cases, the data brokers claim to be able to provide this information within fairly quick time frames, ranging from a few hours to a few days. As a consequence of this information compiled by EPIC and its far-reaching implications on customer security and privacy, OPC is compelled to provide commentary on the Commission's Notice of Proposed Rulemaking (NPRM) as to whether current Commission rules should be modified to

[2] Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115 (filed Aug. 30, 2005) (EPIC Petition).

address this growing problem.

The issue of identity theft and privacy-related infractions is currently in the national forefront. There is rarely a day that goes by where some news article does not report some type of identity theft crime and the hardships that Americans face in trying to correct the egregious damage done by such criminal behavior. Recently, the public has seen instances where companies tasked with protecting sensitive consumer information have been assaulted by computer hackers and thousands of customer accounts have been compromised. The time for more aggressive and protective measures related to CPNI has come. While it is important to find a healthy balance between the protection of confidential customer information and the exercise of commerce in the telecommunications industry, the current FCC Rules implementing FTA §222 are in need of an update that reflects the changing tactics by data brokers and other third parties improperly obtaining this information.

In reviewing the EPIC petition, the applicable Commission rules and the NOPR, OPC notes that what may be required is an expansion of the applicability of the current rules to entities such as data brokers and private investigators to restrict CPNI from these groups and others of that ilk. OPC notes that Congress enacted Section 222 of the Telecommunications Act of 1996, in part, to protect consumer privacy concerns as noted by the statute's language in Section 222(c)(1) which states:

> Except as required by law or with the approval *of* the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision *of* a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

OPC agrees with EPIC that CPNI includes calling history and activity, billing records, and unlisted telephone numbers of service subscribers.' The Act, therefore, prohibits carriers from using, disclosing, or permitting access to CPNI without approval of the customer or as otherwise required by law if the use or disclosure is not in connection with the provided service, or listed as one of the exceptions provided for in Section 222(d). However, some of the Commission rules implementing Section 222 of the Telecommunications Act allow for some ambiguity regarding FTA §222(c)(1) and have unintentionally allowed for other third party interests to surreptitiously access this private customer data for profit.

In example, FCC Rule 64.2005 allows for the disclosure of CPNI data to third parties under a number of exceptions. According to this rule, <u>without previous customer approval</u>, a telecommunications carrier can provide such information for providing or marketing other service offerings to the customer's current carrier or provide that same CPNI to its affiliated entities to offer other classes of service.[3] It may also provide CPNI to third parties for

[3] See FCC Rule §64.2005(a).

installation, repair and maintenance services.[4] Moreover, a wireless carrier may disclose CPNI data to provide local and/or long distance service, vertical services and research on the health effects of wireless service, also, without previous customer approval.[5] The main problem with all of these related exceptions is that there is no clear mechanism by which the wireline or wireless carrier can confirm that the information requested by a third party is for the exceptions noted under FCC Rule 64.2005. Without such verification methods, the carrier is releasing private customer information to any entity that claims to be requiring the data for a legitimate purpose under the Commission rule and federal law.

OPC notes that Texas has enacted stringent verification standards for telephone slamming and cramming, which has, in part, led to a decrease in these types of offenses. One of the reasons for such a reduction in these types of infractions is due to the strict verification methods imposed upon telecommunications carriers prior to a switch in carrier or the imposition of a billed product or service on an invoice to a customer.[6] EPIC claims that data brokers and private investigators have been taking advantage of inadequate verification measures through pretexting, the practice of pretending to have authority to access protected records; through cracking consumers' online accounts with communications carriers; and possibly through dishonest

[4] See FCC Rule §64.2005(c)(1)
[5] See FCC Rule §64.2005(b)(1) and (c)(2).
[6] See P.U.C. Substantive Rules 26.32(d) and (f). See also P.U.C. Substantive Rule 26.130(c).

insiders at carriers.[7] While OPC has not conducted its own studies to support EPICs findings, the frequency and impact of identity crimes related to the unauthorized intrusions into customer privacy rights are on the rise and its impact and costs on consumers and the public at large is undeniable. Thus, OPC supports sensible and effective modification of existing FCC rules to ensure that the practices EPIC alleges are stopped immediately.

How is this to be accomplished? OPC makes the following recommendations:

1. Internally, telecommunications carriers must be required to enact and follow strict Code of Conduct procedures regarding the care, control and disclosure of CPNI data. The FCC Rules should be amended to require carriers to file for approval (either by the FCC or the respective state commissions) procedures specifically designed to maximize the security of customer account information. This would include database security related to hardware and software, restricted access to customer database information to a finite number of individuals and a tracking system that indicates the manner by which any CPNI data was disseminated and by which employee or employees. All employees subject to the care and control of such data should be subject to periodic re-training on the Code of Conduct procedures as well and strict procedures should be put in place regarding employee discipline for unauthorized release of CPNI information to entities not eligible to receive such data. The FCC or the respective state commissions should consider performing some type of compliance auditing on a periodic basis to ensure the effectiveness of such programs.

2. In keeping with the first recommendation, telecommunications carriers that disseminate CPNI pursuant to FTA §222 and FCC Rule 64.2005 should be able to confirm the identity of employees from affiliated carriers requesting such data and also the identity of employees from repair, installation and maintenance entities. Confirmation of such employment helps to limit the universe of persons privy to the CPNI data for that customer and ensures that the information is kept more secure. Further, in the event of a

[7] See EPIC Petition for Rulemaking (August 30, 2005) at 1.

breach of security where it is suspected that internal employees are involved in the alleged CPNI disclosure, it allows for more focused internal investigations to ferret out the violator.

3. Telecommunications carriers should enact measures to tighten customer database information using the most advanced encryption methods and instruct customers on employing better password construction and security. Further, customers should be instructed to frequently change passwords and not to use easily discernible passwords.

4. Telecommunications carriers should work in tandem with state and federal law enforcement personnel to determine whether "pretexting" or any such similar behavior constitute any violation of state and/or federal law. If so, law enforcement should be required to pursue and prosecute alleged violators.

5. OPC recommends that FCC Rule 64.2007 be modified to confirm the customer's identity prior to using the purported approval to use CPNI. This may be accomplished through the use of some type of password or confidential identifying information to reduce the possibility of pretexting.

6. Further, OPC recommends that FCC Rule 64.2007(a)(2) be changed to limit the amount of time that customer approval for use of CPNI can be employed by a telecommunication carrier. After the expiration of that time period, the default position of access to CPNI would then revert to customer non-authorization until approval was once again obtained from the customer or his/her designee pursuant to current FCC regulations.

OPC recognizes that FCC Rule 64.2009 includes some of the safeguards that have been mentioned in the first two recommendations. However, it is incumbent upon the FCC to require carriers to enact the requirements noted in this FCC Rule. The dangers to customers as a result of pretexting and data mining are far too great. OPC acknowledges the FCC's efforts and recognizes its continued commitment toward enforcing existing regulations in

this regard.

II. CONCLUSION

In closing, Texas OPC appreciates the opportunity to present its comments related to this issue on CPNI security. It is imperative that the FCC consider modification of some of its current regulations to address the burgeoning business of improperly obtaining CPNI data. Privacy issues are under assault in many different quarters in our society and as technology advances, more individuals are finding ways to use technology to obtain confidential information. The FCC must keep pace with these technological changes and be aware of what uses CPNI can be employed by some parties for financial gain. As noted, OPC has provided some recommendations for the proposed rulemaking. Such recommendations are by no means all-encompassing and OPC reserves the opportunity to provide further responses to other parties' comments in this proceeding.

Promoting the safety and welfare of all Americans.

April 14, 2006

Respectfully submitted,

Suzi Ray McClellan
Public Counsel
State Bar No. 16607620

_____

Mark Gladney
Assistant Public Counsel
TEXAS OFFICE OF PUBLIC UTILITY COUNSEL

1701 N. Congress Avenue, Suite 9-180
P.O. Box 12397
Austin, Texas 78711-2397
512/936-7500 (Telephone)
512/936-7520 (Facsimile)